THE HIPAA PRIVACY RULE'S RIGHT OF ACCESS AND HEALTH INFORMATION TECHNOLOGY

BACKGROUND AND INTRODUCTION

Since its inception, the HIPAA Privacy Rule's right of an individual to access protected health information (PHI) about him or her held by a covered entity has operated in a primarily paper-based environment. While it has been common for covered entities to create, maintain, and exchange PHI in paper form, an increasing number of covered entities are beginning to utilize new forms of health information technology (health IT), which often involve the transition of PHI from paper to electronic form. Many health care providers, for example, are adopting comprehensive electronic health records (EHRs) to enhance the quality and efficiency of care they deliver. Health IT also may create mechanisms by which individuals can electronically request access to their PHI and by which covered entities can respond by providing or denying access electronically.

An individual's right to access his or her PHI is a critical aspect of the Privacy Rule, the application of which naturally extends to an electronic environment. The Privacy Rule establishes, with limited exceptions, an enforceable means by which individuals have a right to review or obtain copies of their PHI, to the extent it is maintained in the designated record set(s) of a covered entity. The Privacy Rule's specific, yet flexible, standards also address individuals' requests for access and timely action by the covered entity, including the provision of access, denial of access, and documentation. See 45 C.F.R. § 164.524.

Health IT has the potential to facilitate the Privacy Rule's right of access from both an individual's and a covered entity's perspective. Because the right of access operates regardless of the format of the PHI, its application in an electronic environment is similar to that in a paper-based environment. Several provisions, however, such as those related to requests for access, timely action, verification, form or format of access, and denial of access, may apply slightly differently and, thus, require additional consideration. The discussion that follows addresses an individual's right to request access electronically, a covered entity's electronic provision or denial of access and other specific applications of the Privacy Rule that will assist covered entities in tailoring their compliance appropriately.

The guidance also is meant to serve as a stepping stone for covered entities that are considering how an individual's access rights may be fulfilled within an electronic health information exchange environment. To that end, the guidance demonstrates how the Privacy Rule's access standard provides a strong foundation from which covered entities can develop policies and procedures which also meet several of the objectives enumerated in the Individual Access Principle identified within *The Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information*.

REQUESTS FOR ACCESS

The Privacy Rule allows covered entities to require that individuals make requests for access in writing, provided they inform individuals of such a requirement. See 45 C.F.R. § 164.524(b)(1). In addition, the Privacy Rule has always considered electronic documents to qualify as written documents. Thus, the Privacy Rule supports covered entities' offering individuals the option of using electronic means (e.g., e-mail, web portal) to make requests for access.

TIMELY ACTION

The Privacy Rule requires covered entities to respond to requests for access in a timely manner. Except as otherwise specified, the Privacy Rule requires the individual be notified of the decision within 30 days of the covered entity's receipt of the request. See 45 C.F.R. § 164.524(b)(2)(i). While the Privacy Rule establishes the 30 days as an outside limit, it does not preclude covered entities from responding sooner. Indeed, a covered entity may have the capacity through the use of some electronic systems to provide automated access to an individual's PHI or respond to requests with immediate access, twenty-four hours a day. Not all electronic systems, however, may allow for the provision of immediate access, and the covered entity's response time-frame will normally depend, in part, on its system capacity.

As in a paper-based system, other factors also will impact a covered entity's response time in an electronic environment. For example, the Privacy Rule's 30 day parameter was originally conceptualized to allow covered entities sufficient time to accommodate normal business functions (e.g., interpretation of test results), as well as those unusual circumstances that might delay a response (e.g., reporting suspected child abuse). Similar allowances may be necessary in an electronic health information environment as well.

As a practical matter, individuals might expect, when making a request of a technologically sophisticated covered entity, that their requests could be responded to instantaneously or well before the current required time-frame. This might be the case, for example, when access is provided through a direct view or portal into a health care provider's EHR. Providing more timely access than the Privacy Rule requires may be a means by which covered entities distinguish themselves within the market.

PROVISION OF ACCESS

WHO MAY EXERCISE THE RIGHT OF ACCESS?

Individuals and Personal Representatives. While the Privacy Rule's right of access belongs primarily to the individual who is the subject of the PHI, the Privacy Rule also generally requires that persons who are legally authorized to act on behalf of the individual regarding health care matters be granted the same right of access. See 45 C.F.R. § 164.502(g)(1). The Privacy Rule defers to state law to determine when a person has the legal authority to act on behalf of an individual with regard to health care matters. Health care powers of attorney and parental rights, for example, are two legal bases by which state law may be determinative of a person's authority to act on behalf of an individual.

The Privacy Rule's personal representative requirement ensures that certain people will have access to an individual's PHI when the individual is incapacitated or otherwise unable to exercise the right of access on his or her own behalf. The Privacy Rule would require that covered entities grant personal representatives with the right of access on behalf of an individual in an electronic environment, just as they do today with regard to paper-based information. Covered entities will want to make sure, however, that they have the capacity to identify, authenticate, and properly respond to requests from these individuals, whether electronically or otherwise, as the Privacy Rule requires.

Verification. The Privacy Rule requires covered entities to develop and implement reasonable policies and procedures to verify the identity of any person who requests PHI, as well as the authority of the person to have access to the information, if the identity or authority of the person is not already known. See 45 C.F.R. § 164.514(h)(1). These verification requirements apply to individuals who request access to their PHI that is maintained in a designated record set. The Privacy Rule refrains from defining specific or technical verification requirements and largely defers to the covered entity's professional judgment and industry standards to determine what is reasonable and appropriate under the circumstances.

Verification may be obtained either orally, or in writing (which may be satisfied electronically), so long as the requisite documentation, statements or representations are obtained where required by a specific Privacy Rule disclosure provision, and that the appropriate steps are ultimately taken to verify the identity and authority of individuals or personal representatives who are otherwise unknown. Therefore, covered entities that receive and/or respond to access requests electronically should revisit their verification and documentation policies and procedures to ensure that they are reasonable in light of the electronic environment within which they are operating.

CONTENT - DESIGNATED RECORD SETS

An individual's right of access generally applies to the information that exists within a covered entity's designated record set(s), including: (1) a health care provider's medical and billing records, (2) a health plan's enrollment, payment, claims adjudication, and case or medical management record systems, and (3) any information used, in whole or in part, by or for the covered entity to make decisions about individuals. A record is any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the covered entity. See 45 C.F.R. § 164.501 (definition of "designated record set").

Covered entities that use electronic records (e.g., EHRs or electronic claims systems) will want to remain cognizant that the right of access applies regardless of the information's format. The term "designated record set," therefore, cannot be limited to information contained in an electronic record, but also will include any non-duplicative, electronic or paper-based information that meets the term's definition. While overlap may initially exist between electronic and paper-based record sets, covered entities will likely find their access-related obligations to be less time and labor intensive the more PHI they convert to being electronic.

Further, a covered entity that utilizes a business associate to maintain or otherwise operate its electronic records will want to ensure the business associate is obligated to share non-duplicative information pursuant to electronic access requests. The same would be true if a health information organization (HIO), as a business associate, maintains an electronic repository of some or all of a covered entity's PHI.

FORM OR FORMAT OF ACCESS PROVIDED

The Privacy Rule requires covered entities to provide access to the PHI in the form or format requested by the individual, if it is readily producible in such form or format. If the PHI is not readily producible in the form or format requested, access must be provided in a readable hard copy form, or in the alternative, some other form or format as agreed to by the covered entity and the individual. The covered entity also may provide the individual with a summary of the PHI or may provide an explanation of the PHI which has been provided, so long as the individual agrees to the alternative form and associated fees. See 45 C.F.R. § 164.524(c)(2).

To the extent individuals request that access to their PHI be provided in an electronic form or format, covered entities' utilization of electronic records will likely increase the amount of PHI that is "readily producible" in electronic form, thereby benefiting both the requesting individual, as well as the covered entity:

> Electronic access may provide individuals with more timely access to more information in a more convenient manner. For example:
>
> - Electronic copies of PHI may be downloaded to USB thumb-drives or copied to compact discs relatively quickly and may provide individuals with a more convenient means of transporting and maintaining the information.

- EHRs may enable covered entities to offer individuals an immediate and ongoing view into the covered entity's designated record set(s), either through a personal health record (PHR) or otherwise, while limiting the time, expense, and labor that may be required otherwise in order to provide access to the individual.

Electronic access also may be a means by which covered entities can limit the time, resources and other expenses required to provide the individual with access.

- Electronic copies of PHI that are downloaded to USB thumb-drives or copied to compact discs may require less labor and overhead than access to paper records would require.
- Covered entities may find that providing individuals with electronic access to PHI could save them time and resources by limiting, if not eliminating, the need to provide hard copies of the information or some other, more expensive, form or format.
- Providing such "readily producible" electronic access may have the secondary effect of enhancing their communication with individuals, which may in turn, lead to improved quality of care and strengthened consumer satisfaction.

The right of access also affords covered entities the option of making alternative agreements with individuals as to the form or format of access provided. If, for example, a covered entity's default administrative safeguards policies and procedures limit the provision of electronic access to stand-alone devices and secure, web-based portals, and an individual requests access via electronic mail (e-mail), the Privacy Rule would permit alternative agreements which satisfy both parties, so long as reasonable safeguards are otherwise in place.

To the extent that individuals request access to their PHI in hard-copy form, the covered entity must provide such access, even if the information is stored in an electronic record.

DENIAL OF ACCESS

GROUNDS FOR DENIAL

The Privacy Rule contemplates circumstances under which covered entities may deny an individual access to PHI and distinguishes those grounds for denial which are reviewable from those which are not.

Unreviewable grounds for denial are: situations involving (i) psychotherapy notes, information compiled for use in legal proceedings, and certain information held by clinical laboratories; (ii) certain requests which are made by inmates of correctional institutions; (iii) information created or obtained during research that includes treatment if certain conditions are met; (iv) denials permitted by the Privacy Act; and (v)

information obtained from non-health care providers pursuant to promises of confidentiality. See 45 C.F.R. § 164.524(a)(2).

Reviewable grounds for denial are: (i) disclosures which would cause endangerment of the individual or another person; (ii) situations where the PHI refers to another and disclosure is likely to cause substantial harm; and (iii) requests made by a personal representative where disclosure is likely to cause substantial harm. See 45 C.F.R. § 164.524(a)(3).

Implementation of Denial

The Privacy Rule further requires that denials of access be timely, written, provided to individuals in plain language, with a description of the basis for denial, and if applicable, contain statements of the individual's rights to have the decision reviewed and how to request such a review. In addition, the notice of denial must inform the individual of how complaints may be filed with the covered entity or the Secretary of HHS. If access to some of the PHI is denied, the covered entity must, to the extent possible, give the individual access to any other PHI requested, after excluding the PHI to which the covered entity has a ground to deny access. See 45 C.F.R. § 164.524(d)(1).

A covered entity may satisfy the Privacy Rule's writing requirement for denials electronically, though its denial still must be based on the grounds identified by the Privacy Rule, and must comply with each of the Privacy Rule's procedural requirements. In cases where the covered entity is able to receive and process a request for access by the individual electronically and provide access in an electronic format, the denial of the request, in whole or in part, may also be done electronically. As emphasized above, the form of the denial does not change the covered entity's obligations regarding the basis for the denial or the content of the notification to the individual. However, where the covered entity provides individuals with electronic access to some or all of their health information, through a PHR or similar means, and the access is available to the individual at any time and without a request, it becomes more difficult to determine whether a denial of access has occurred and when notice to the individual is required. For example, the requirements in the Privacy Rule are flexible enough to permit a covered entity to notify the individual in advance of the types of PHI to which it intends to deny access and for which the Privacy Rule does not provide a right of review. See 45 C.F.R. § 164.524(a)(2). Such advance notification would not be appropriate, however, for other types of PHI to which a covered entity may deny access because the denial must be based on the specific exercise of professional judgment by a licensed health care professional and are subject to the individual's right to request a review of the denial by another licensed health care professional. In these cases, the individual must be aware of the fact that he or she has been denied access to certain information for which the individual has a right to request a review. See 45 C.F.R. § 164.524(a)(3). The covered entity's policies and procedures for the provision of electronic access must appropriately provide for these individualized grounds for denial of access.

FREQUENTLY ASKED QUESTIONS

Q1: In an electronic health information exchange environment, what is a designated record set for purposes of an individual's right of access under the HIPAA Privacy Rule?

A1: To the extent covered entities maintain their own electronic records systems, their choice to link those systems to a network for electronic health information exchange purposes would not necessarily change the status of information maintained within their designated record sets. That is, information that meets the definition of a designated record set remains part of the designated record set even if that information is linked to a network. See 45 C.F.R. § 164.501 (definition of "designated record set"). Covered entities should be aware, however, that whatever information they import into their electronic records via a network may become an integrated part of their designated record set(s). Network participation alone, however, would not make all other information about the individual that is accessible through the network part of a covered entity's designated record set. Thus, the ability to link to information through a network does not obligate a covered entity to provide access to the designated record set of another entity participating in the network.

Q2: How would a covered entity or health information organization (HIO), acting on its behalf, know if someone were a personal representative for the purpose of granting access under the HIPAA Privacy Rule?

A2: The Privacy Rule's verification standard requires that covered entities develop and implement reasonable policies and procedures to verify the identity and authority of such persons, if otherwise unknown to them, before granting them access to protected health information (PHI). See 45 C.F.R. § 164.514(h). Once verified, the personal representative can then be given the appropriate credentials for authentication and access through an electronic system. The Privacy Rule allows covered entities to rely on their professional judgment, as well as industry standards, in designing reasonable verification and authentication processes.

The Privacy Rule permits a covered entity to assign this function to a HIO, acting as its business associate, so long as the relevant standards are complied with. For example, a covered entity could use the HIO to assign the appropriate credentials and authenticate personal representatives, and any others, seeking access to PHI.

Q3: How may judgments be made electronically about denial of access under the HIPAA Privacy Rule?

A3: The Privacy Rule differentiates between two types of denial, reviewable and unreviewable. See 45 C.F.R. § 164.524(a)(2), (3). As to the unreviewable grounds for denial, there are essentially two decisions a covered entity will need to make with respect to electronic access: 1) whether it may deny access based on one or more of the grounds identified by the Privacy Rule; and 2) how to implement such decisions categorically in the electronic environment.

A covered entity may decide, for example, to categorically deny access to certain types of information to which no access right exists, such as psychotherapy notes. The Privacy Rule would permit denial without review, and a case-by-case judgment would not be necessary. Similarly, the covered entity may make such a system-wide decision with respect to other types of protected health information where the Privacy Rule permits an unreviewable denial of access.

In contrast, reviewable grounds for denial of access require decisions be made on a case-by-case basis through the professional judgment of licensed health care providers. Professional judgment also would be required if individuals exercise their right to appeal a denial of access made on reviewable grounds. As computer logic cannot be a substitute for professional judgment in these cases, these types of activities cannot be carried out categorically or in an automated way. Neither could these decisions be delegated to a health information organization (HIO), unless a licensed health care professional at the HIO were assigned the task of making the access determinations.